在SNMP v2和v3配置中，排除Nexus 5k、7k和9K中的OID

目錄

簡介

本文檔介紹如何在SNMP v2和v3配置中排除Nexus 5k、7k和9K中的OID。

必要條件

需求

思科建議您在實施對象識別符號(OID)排除項之前瞭解以下主題：

- 熟悉簡單網路管理協定(SNMP)
- 訪問裝置配置模式
- 瞭解要排除的OID
- 瞭解SNMP社群和使用者配置

採用元件

本文檔中的資訊基於對以下Nexus型號進行的實驗室測試：

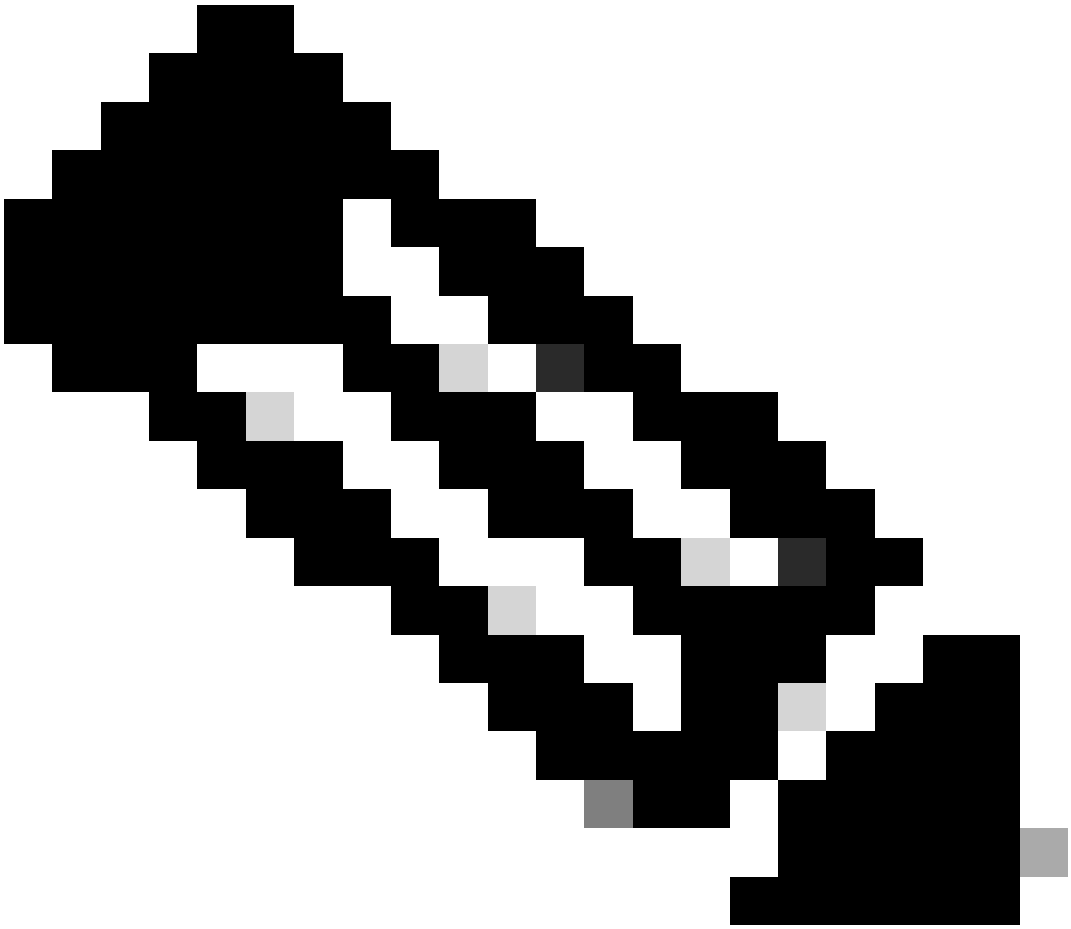
- Nexus 5k
- Nexus 7k
- Nexus 9k

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

在SNMP的世界中，您經常會遇到管理資訊庫(MIB)樹的解析遇到障礙的情況，在特定OID處停頓有

時會導致窗口超時或類似問題。當對有問題的OID進行持續輪詢時，會觸發既不必要也不具影響的警報時，就會出現另一個常見問題。擺脫這些情況的一種可能方法是建立排除，指示裝置跳過該特定OID並繼續執行MIB結構的其餘部分。透過引導裝置繞過有問題的OID並繼續執行MIB結構的其餘部分，您可以促進MIB樹的平滑流動。



注意：請注意，此排除項可能會影響我們從MIB樹中讀取資料的方式，這一點很重要。在進行這些排除之前，請謹慎行事，並確保OID的必要性。

雖然排除OID通常在聚合服務路由器(ASR)/Catalyst交換機(CAT)/整合服務路由器(ISR)等裝置中追求簡單流程，但由於缺少檢視，在Nexus裝置中應對此挑戰顯得更為複雜。本文將介紹一種創新方法，即引入角色並將其對映到社群/使用者，介紹一種在Nexus 5k、7k和9K裝置上的SNMP v2和v3配置中排除OID的解決方案。

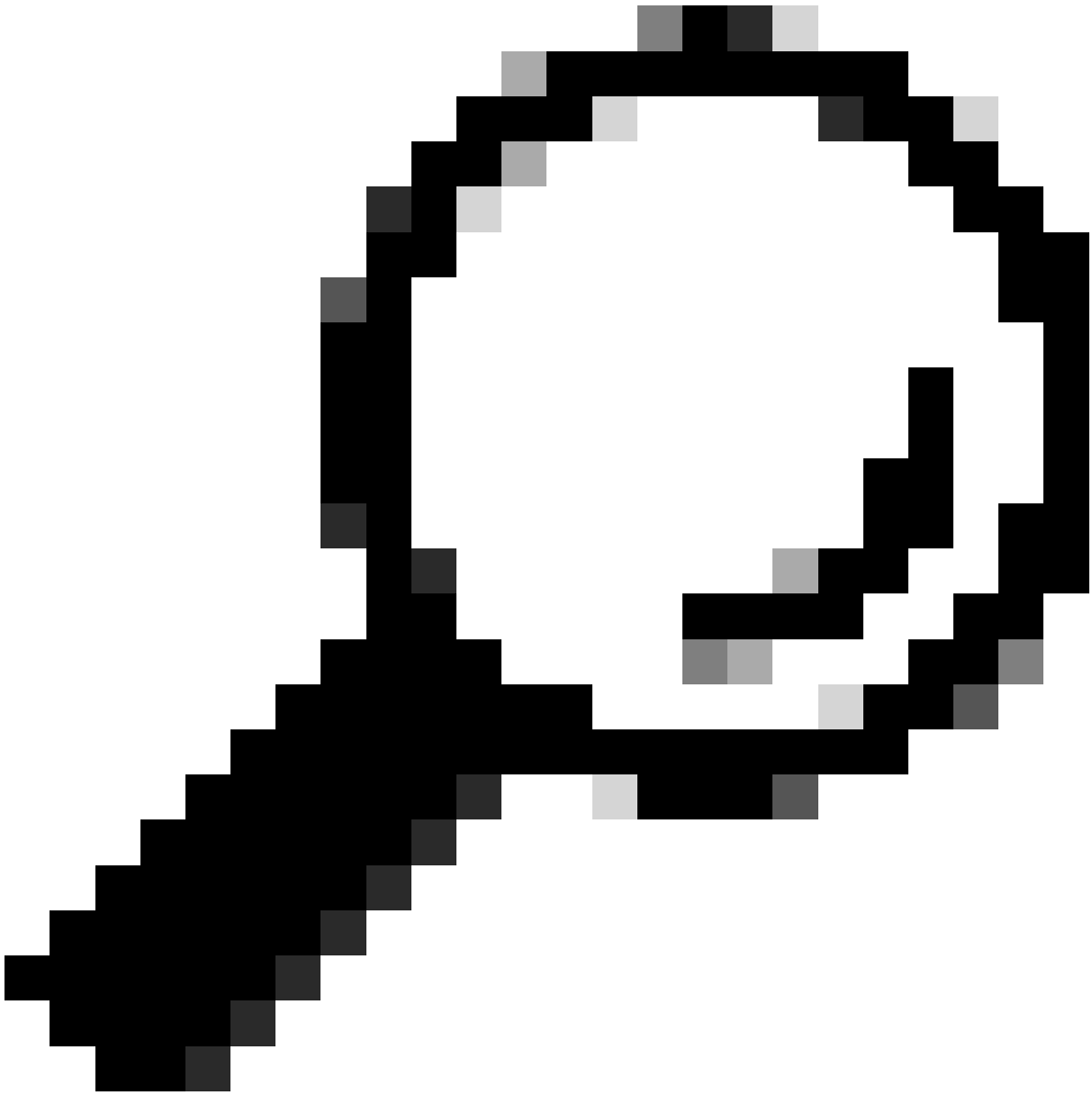
基本步驟

訪問配置模式：

```
#conf t
```

定義OID排除的角色：

```
#role name <name_of_role>
#rule 1 permit read feature snmp
#rule 2 deny {read/ read-write} oid <oid_you_want_to_exclude>
```



提示：{read/read-write}允許您在「讀取」和「讀取/寫入」SNMP操作之間進行選擇。「讀取」操作通常涉及檢索資訊，而「讀取/寫入」操作同時涉及檢索和修改資訊。您可以根據自己的偏好選擇讀取/讀取/寫入。

離開組態設定模式：

```
#exit
```

將組態套用至SNMP社群/使用者。

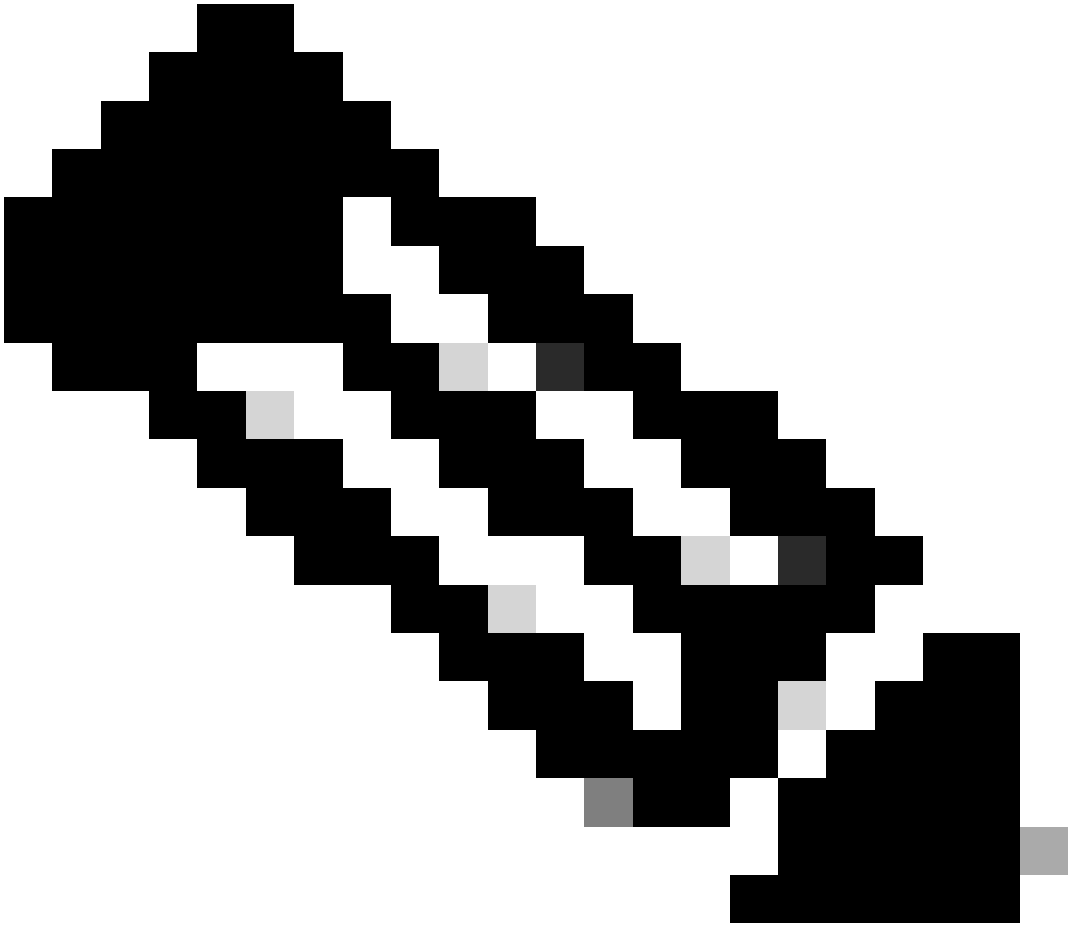
對於SNMPv2：

```
#snmp-server community <name_of_community_you_want_to_map> group <name_of_role>
```

對於SNMPv3：

```
#snmp-server user <user_to_map_with> <name_of_role> auth {sha/md5} <authentication_password> priv {aes/
```

組態



注意：本示例包括對OID 1.3.6.1.2.1.2.2.1.3(ifType)的排除。請務必將ifType OID取代為您要排除的OID。

定義排除OID ifType的角色：

```
switch#
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# role name deny_oid
switch(config-role)# rule 1 permit read feature snmp
switch(config-role)# rule 2 deny read oid 1.3.6.1.2.1.2.2.1.3
switch(config-role)# exit
switch(config)# exit
switch# sh role name deny_oid
Role: deny_oid
  Description: new role
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)
```

```
  ------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ------------------------------------------------------------------
  2       deny    read        oid                 1.3.6.1.2.1.2.2.1.3
  1       permit  read        feature             snmp
switch#
```

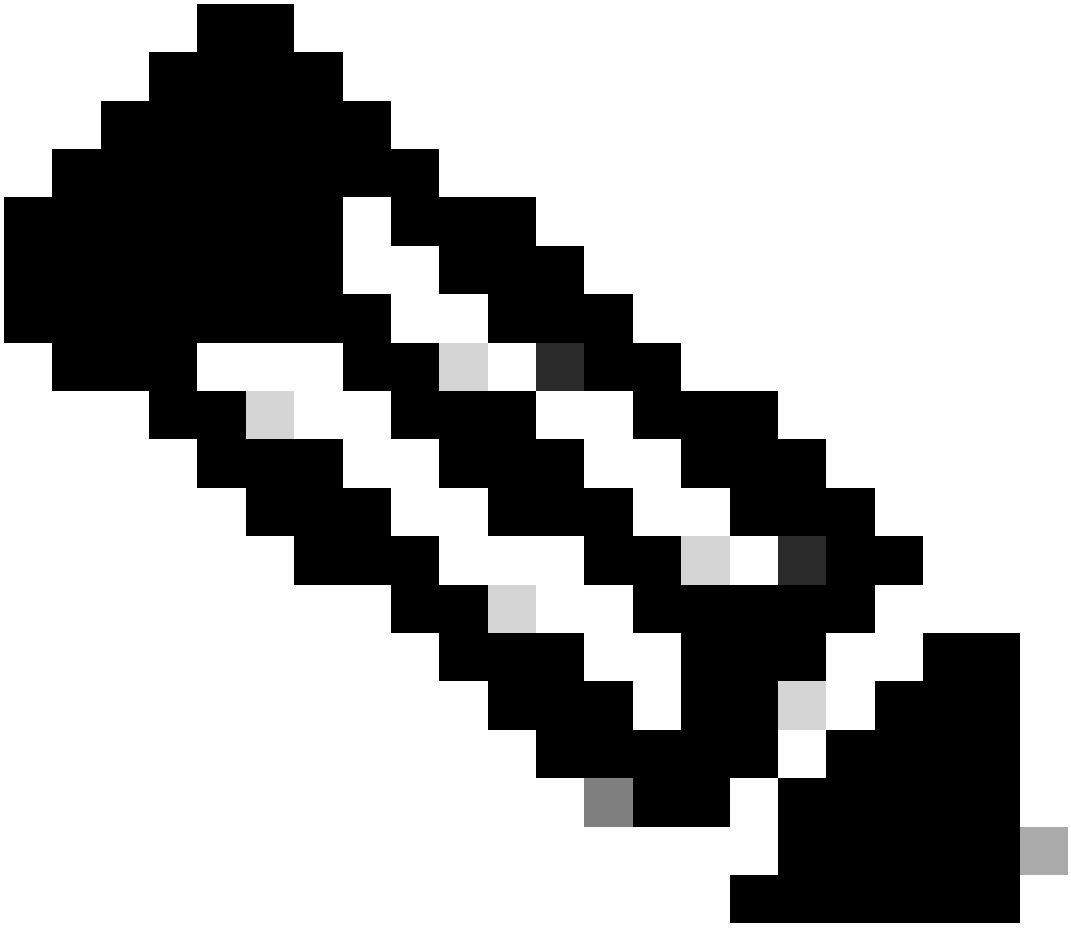
建立具有deny_oid角色的SNMPv2社群：

```
switch(config)# snmp-server community snmpv2user group deny_oid switch(config)# exit switch# sh snmp co
```

正在建立具有**deny_oid**角色的SNMPv3使用者：

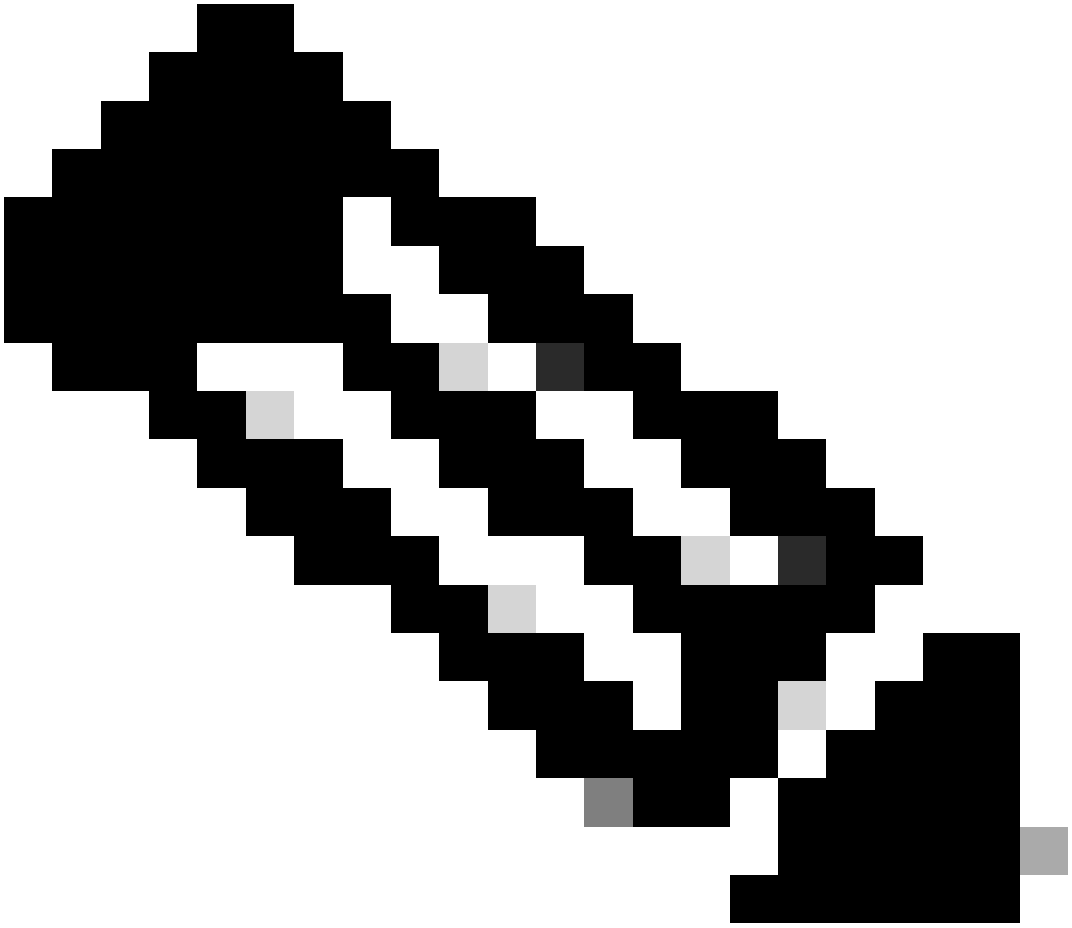
```
switch# config t Enter configuration commands, one per line. End with CNTL/Z. switch(config)# snmp-serv
```

驗證



注意：測試使用者「trial」用於檢查ifType OID的輪詢。其餘的使用者都對映了**deny_oid**角色，並且如圖所示，該角色未顯示ifType OID的資料。

不排除的SNMPwalk：

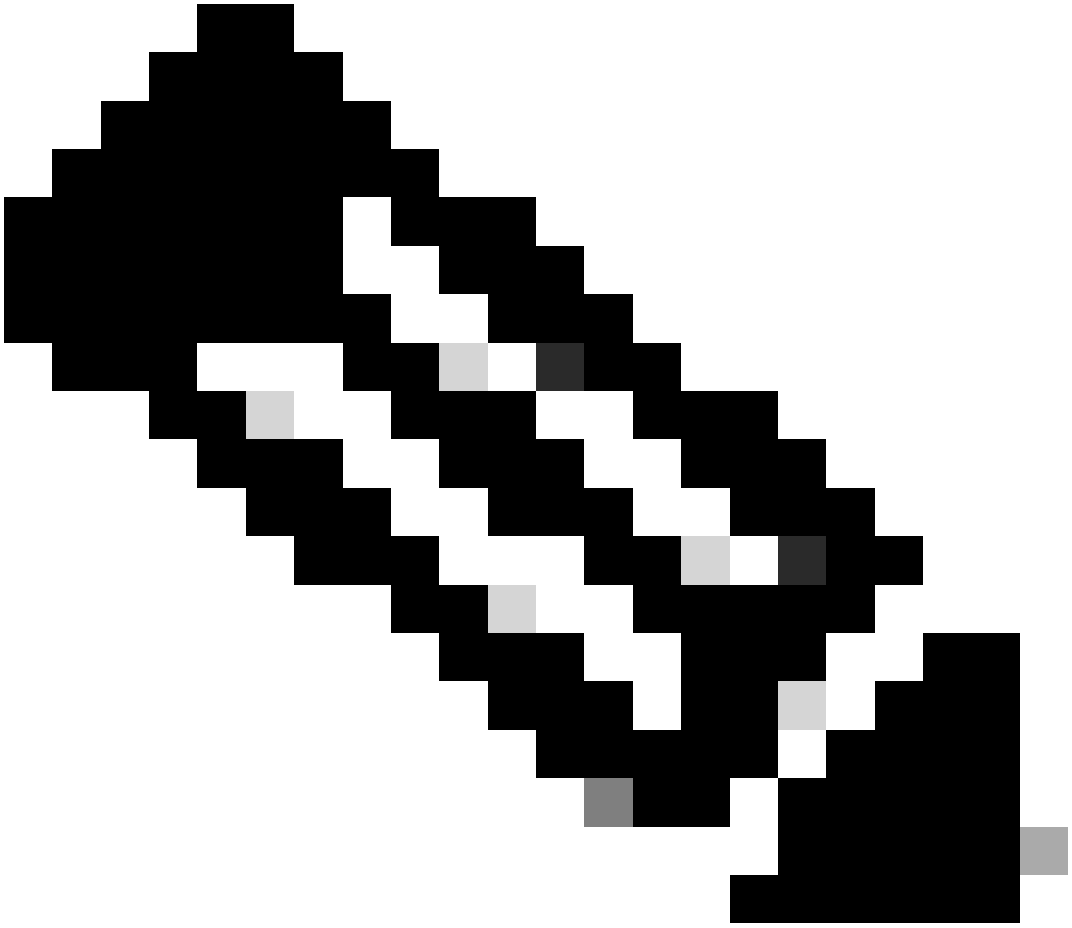


注意：在本文中，a.b.c.d用於代替裝置的IP地址。

```
[root@user ~]# snmpwalk -v2c -c trial a.b.c.d 1.3.6.1.2.1.2.2.1.3 IF-MIB::ifType.83886080 = INTEGER: et
```

具有已排除OID的SNMPv2的SNMPwalk：

```
[root@user ~]# snmpwalk -v2c -c snmpv2user a.b.c.d 1.3.6.1.2.1.2.2.1.3 IF-MIB::ifType = No Such Object
```



注意：建立了一個新使用者「trialv3」來演示不排除OID的輪詢。

不排除OID的SNMPwalk：

```
[root@user ~]# snmpwalk -v3 -u trialv3 -l authPriv -a sha -A 'password!123' -x aes -X 'password!123' a.
```

具有已排除OID的SNMPv3使用者的SNMPwalk：

```
[root@user ~]# snmpwalk -v3 -u snmpv3user -l authPriv -a sha -A 'password!123' -x aes -X 'password!123'
```

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。